ISA INFINITY

PARTNER BATTLE CARD: Minimum requirements **RADAR** and on-boarding

Ensure your client's satisfaction

How is the service set up?

Unlike many other cybersecurity services, the on-boarding process for **RADAR** is simple. After placing an order, the ISA team will reach out to the partner to provide a list of the IP's that the client wants to scan for vulnerabilities. After the order is completed, ISA will connect with a contact at the client organization to confirm the necessary firewall policies are in place:

Predefined Firewall policies are checked

Virtual scanner is deployed in client network with the help of the ISA team

IP's – provided by partner – are assigned to scanner

RADAR service goes live and scanning starts

Critical insights and reports at your fingertips.

Organizations protected by ISA's SOC-as-a-Service solutions have secure access to a dynamic portal where they can access easy to understand insights through dashboards and monthly reports. The client contact is provided with login credentials to access their ISA portal.

We are here to help.

Successful implementation of the **RADAR** service and your client's satisfaction relies on a clear understanding of the on-boarding process and minimum requirements for the services. Reach out to infinity@isacybersecurity.com or Ingram Micro for more information.

Do you have more questions?

If you need more information on the minimum requirements for the successful deployment of the service, don't hesitate to reach out to infinity@isacybersecurity.com.

Minimum system requirements.

+ CPU: 4 - 2 GHz Cores
+ Memory: 4 GB RAM
+ Disk Space: 30 GB
+ OS: Windows Server 2012, Server 2012 R2, Server 2016, and Windows 10 or Linux (Red Hat ES 6/7, CentOS 6/7, Oracle Linux 6/7, Ubuntu 12.04/12.10/13.04/13.10/14.04/16.04/18.04)

Recommended system requirements.

+ CPU: 8 - 2 GHz Cores
+ Memory: 16 GB RAM
+ Disk Space: 80 GB
+ OS: Windows Server 2016 or Linux (Red Hat ES 7, CentOS 7, Oracle Linux 7, Ubuntu 18.04)

Firewall policies.

Please ensure the following policies are in place with your client's firewall ports.

+ Allow Incoming TCP Port 8834 from 66.70.213.171
+ Allow Outgoing TCP Port 443 to 66.70.213.171
+ Allow Outgoing TCP Port 25
+ Allow Outgoing UDP Port 53
+ Allow All Outgoing Traffic from Nessus Scanner (installed in client's network) to all internal

Learn more about the ISA Infinity Partner Program at www.isacybersecurity.com/cn-partners-infinity | Register a deal via infinity@isacybersecurity.com | Contact Ingram Micro for more information via CyberSecurityCanada@ingrammicro.com

INGRAM MICRO®